KRİPTO PARA VE BLOKZİNCİR ADLİ TAKİBİ

Cüzdandan Faile: On-Chain Analizin Teknik, Metodolojik ve Hukuki Boyutları

Cryptocurrency and Blockchain Forensic Tracing: Technical, Methodological and Legal Dimensions of On-Chain Analysis from Wallet to Perpetrator

Derleme Makale / Review Article

Dr. Burak Olgun

burakolgun@solutionhome.net

Solution Home Bilişim Tekn. ve Dan. Hizm., İstanbul

Blokzincir Adli Analizi • On-Chain İz Sürme • Kümeleme • Mixer • Kara Para Aklama • Kripto Varlık • Delil Zinciri

ÖZET

Kripto varlıkların sağladığı sözde-anonimlik (pseudonymity), suç gelirlerinin aklanması, fidye yazılımı, dolandırıcılık ve yaptırım kaçakçılığı gibi eylemlerde tercih edilen bir araç hâline gelmiştir. Buna karşılık, çoğu blokzincirin genel (public) ve değiştirilemez (immutable) defter yapısı, geleneksel finansal sistemlerde bulunmayan bir adli takip olanağı doğurmaktadır. Bu makale, kripto varlık işlemlerinin adli bilişim yöntemleriyle izlenmesini üç boyutta ele almaktadır: (i) blokzincirin adli temelleri ve on-chain analizin metodolojisi (kümeleme, ortak girdi sahipliği sezgiseli, etiketleme ve grafik tabanlı iz sürme); (ii) suç faillerinin izi gizlemek için kullandığı karıştırıcı (mixer), zincirler arası köprü, gizlilik odaklı coin ve katmanlama (layering) teknikleri; (iii) elde edilen bulguların delil değeri, delil zincirinin korunması ve Türk hukuku ile uluslararası düzenlemeler karşısındaki konumu. 2025 yılı verileri ışığında yasadışı kripto ekonomisinin ölçeği tartışılmakta, Şubat 2025 tarihli Bybit soygunu somut bir vaka olarak incelenmektedir. Türkiye bağlamında 7518 sayılı Kanun ile getirilen kripto varlık hizmet sağlayıcı rejimi, MASAK yükümlülükleri ve TCK m. 282 çerçevesi değerlendirilmekte; bilirkişilik uygulaması için yöntemsel öneriler sunulmaktadır. Çalışma, on-chain analizin güçlü bir soruşturma aracı olduğunu, ancak yalnızca zincir-dışı (off-chain) kimlik verisiyle birleştirildiğinde ve delil zinciri titizlikle korunduğunda mahkeme önünde güvenilir bir delile dönüştüğünü ortaya koymaktadır.

Anahtar Kelimeler: *blokzincir adli analizi, on-chain iz sürme, kümeleme, ortak girdi sahipliği sezgiseli, mixer, kara para aklama, kripto varlık, delil zinciri, MASAK, Bybit.*

ABSTRACT

The pseudonymity offered by crypto assets has made them a preferred instrument for money laundering, ransomware, fraud and sanctions evasion. Conversely, the public and immutable ledger structure of most blockchains creates a forensic traceability that is absent in traditional financial systems. This article examines the forensic tracing of crypto-asset transactions along three axes: (i) the forensic foundations of the blockchain and the methodology of on-chain analysis (clustering, the common-input-ownership heuristic, attribution and graph-based tracing); (ii) the obfuscation techniques used by offenders, including mixers, cross-chain bridges, privacy coins and layering; and (iii) the evidentiary value of the findings, the preservation of the chain of custody, and their standing under Turkish law and international

burakolgun.com

regulation. Drawing on 2025 data, the scale of the illicit crypto economy is discussed and the February 2025 Bybit heist is analysed as a concrete case. In the Turkish context, the crypto-asset service provider regime introduced by Law No. 7518, the obligations under the Financial Crimes Investigation Board (MASAK) and the framework of Article 282 of the Turkish Penal Code are evaluated, and methodological recommendations for expert-witness practice are provided. The study concludes that on-chain analysis is a powerful investigative tool, but becomes reliable courtroom evidence only when combined with off-chain identity data and when the chain of custody is rigorously preserved.

Keywords: *blockchain forensics, on-chain tracing, clustering, common-input-ownership heuristic, mixer, money laundering, crypto asset, chain of custody, MASAK, Bybit.*

burakolgun.com

1. Giriş

Kripto varlıklar, 2008 yılında Bitcoin'in kavramsal temelini oluşturan çalışmayla birlikte (Nakamoto, 2008) ortaya çıktıklarında, merkezî bir otoriteye ihtiyaç duymadan değer transferi vaadi taşıyordu. Bu vaadin teknik karşılığı, işlemlerin bir aracı kuruma değil, dağıtık bir ağ tarafından ortaklaşa tutulan ve kriptografik olarak birbirine bağlanan bir deftere (ledger) kaydedilmesidir. Aradan geçen süreçte kripto varlıklar hem meşru bir yatırım ve ödeme aracına hem de suç gelirlerinin taşınması, gizlenmesi ve aklanması için başvurulan bir kanala dönüşmüştür. Bu ikili nitelik, adli bilişim disiplini açısından kendine özgü bir gerilim yaratmaktadır: Suçlular anonimlik arayışıyla bu araçlara yönelirken, aynı sistemin şeffaf defter mimarisi, geleneksel bankacılıkta erişilmesi güç olan bir izlenebilirlik sunmaktadır.

Kamuoyunda yaygın olan 'kripto para tamamen anonimdir' algısı, teknik gerçekle örtüşmez. Bitcoin ve benzeri açık defterli ağlarda her işlem, kalıcı ve herkese açık biçimde kayıt altına alınır; kullanıcı kimlikleri doğrudan görünmese de, adresler ve işlemler arasındaki ilişkiler analiz edilebilir. Bu nedenle literatürde daha isabetli bir kavram olarak **sözde-anonimlik** (pseudonymity) kullanılır: Kimlik bir takma adın (adresin) ardında gizlidir, ancak takma ad ile gerçek kimlik arasındaki bağ, yeterli veri ve yöntemle kurulabilir. Meiklejohn ve arkadaşlarının (2013) öncü çalışması, Bitcoin işlemlerinin kümelenerek gerçek dünya aktörlerine bağlanabileceğini deneysel olarak göstermiş ve modern blokzincir adli analizinin temelini atmıştır.

Yasadışı kripto ekonomisinin ölçeği, son yıllarda hızla büyümüştür. Blokzincir analiz şirketi Chainalysis'in 2026 tarihli raporuna göre, 2025 yılında yasadışı adreslerin aldığı toplam tutar en az 154 milyar dolara ulaşmış; bu rakam bir önceki yıla göre yaklaşık %162 artış göstermiştir (Chainalysis, 2026). Aynı raporda, yasadışı hacmin %84'ünün artık sabit-değerli kripto varlıklar (stablecoin) üzerinden gerçekleştiği ve yaptırım kapsamındaki aktörlerin aldığı değerin yıllık bazda %694 arttığı belirtilmektedir. Buna karşın, yasadışı işlemlerin tüm kripto işlem hacmi içindeki payı hâlâ %1'in altındadır; yani sorun, oransal büyüklüğünden çok mutlak hacmi ve suçun niteliği bakımından önemlidir.

Bu tablo, kolluk kuvvetleri, savcılıklar, düzenleyici kurumlar ve özel sektör uyum birimleri için blokzincir adli analizini vazgeçilmez bir yetkinlik hâline getirmiştir. Ancak on-chain verinin soruşturmada ve yargılamada kullanılabilmesi, salt teknik beceriyle sınırlı değildir; elde edilen bulguların hukuka uygun biçimde toplanması, bütünlüğünün korunması ve mahkeme önünde anlaşılır biçimde sunulması gerekir. Türkiye'de 2 Temmuz 2024 tarihli Resmî Gazete'de yayımlanan 7518 sayılı Kanun ile kripto varlık hizmet sağlayıcıları düzenlemeye tabi kılınmış ve MASAK mevzuatı kapsamında finansal kuruluş statüsüne yaklaştırılmıştır; bu gelişme, adli takip pratiğinin hukuki zeminini önemli ölçüde değiştirmektedir.

Makalenin geri kalanı şu şekilde düzenlenmiştir. İkinci bölüm, blokzincirin adli açıdan önem taşıyan temel yapı taşlarını ve sözde-anonimlik kavramını ele alır. Üçüncü bölüm, on-chain analizin metodolojisini; dördüncü bölüm, failin kullandığı gizleme tekniklerini inceler. Beşinci bölüm Bybit soygununu vaka olarak çözümler; altıncı bölüm 2025 yılı yasadışı ekonomisinin görünümünü verir. Yedinci bölüm delil zinciri ve adli süreç, sekizinci bölüm hukuki çerçeve, dokuzuncu bölüm Türkiye bağlamı üzerinedir. Onuncu bölüm zorlukları ve

burakolgun.com

önerileri, on birinci bölüm sonucu içerir. Çalışma boyunca, herhangi bir gerçek soruşturma dosyasına veya kişiye atıf yapılmamış; kamuya açık raporlar ve akademik kaynaklar temel alınarak yalnızca teknik ve hukuki farkındalık amaçlanmıştır.

2. Blokzincirin Adli Temelleri ve Sözde-Anonimlik

Blokzincir adli analizini anlamak için, öncelikle bu teknolojinin adli açıdan hangi izleri ürettiğini kavramak gerekir. Bir blokzincir, işlemleri kronolojik olarak sıralayan ve her bloğu bir öncekinin kriptografik özetiyle (hash) birbirine bağlayan bir veri yapısıdır. Bu bağlanış, defterin geçmişe dönük olarak değiştirilmesini pratikte olanaksız kılar; bir bloğun içeriği değiştirildiğinde onu izleyen tüm blokların özetleri geçersiz hâle gelir. Adli bilişim açısından bu özellik kritiktir: Defterin **değiştirilemezliği** (immutability), bir kez kaydedilmiş işlemin sonradan tahrif edilemeyeceği anlamına gelir ve bu, delilin bütünlüğü için doğal bir güvence sağlar.

2.1. Adres, İşlem ve Defter Yapısı

Kripto varlık sisteminde kullanıcılar, gerçek kimlikleriyle değil, açık anahtar kriptografisine dayanan **adresler** üzerinden işlem yapar. Bir adres, kabaca, kullanıcının özel anahtarından (private key) türetilen ve fonların gönderilebileceği bir hedefi temsil eden alfasayısal bir dizidir. İşlemler, bu adresler arasındaki değer transferlerini tanımlar ve ağ tarafından doğrulandıktan sonra deftere yazılır. Bir kullanıcının tek bir adresle sınırlı olmaması, aksine yüzlerce hatta binlerce adres üretebilmesi, adli analizi hem zorlaştıran hem de zenginleştiren bir olgudur; çünkü bu adresler arasındaki bağlantılar, analiz için değerli sinyaller taşır.

İki temel muhasebe modeli, adli yaklaşımı doğrudan etkiler. Bitcoin'in kullandığı **UTXO modeli** (Unspent Transaction Output — harcanmamış işlem çıktısı), her fon parçasını ayrı bir 'çıktı' olarak ele alır; bir işlem, önceki çıktıları girdi olarak tüketir ve yeni çıktılar üretir. Bu yapı, fonların adeta işaretlenmiş banknotlar gibi izlenebilmesine olanak tanır ve adli açıdan bir avantajdır. Buna karşın Ethereum'un kullandığı **hesap modeli** (account model), her adresin bir bakiye tuttuğu ve akıllı sözleşmelerin (smart contract) çalıştığı bir yapıdır; burada fonlar bakiyeler içinde birbirine karışır ve doğrudan 'parça' takibi UTXO'daki kadar berrak değildir. Tablo 1, iki modelin adli açıdan karşılaştırmasını özetlemektedir.

Tablo 1. UTXO ve Hesap Modelinin Adli Takip Açısından Karşılaştırması

Özellik	UTXO Modeli (Bitcoin)	Hesap Modeli (Ethereum)
Temel birim	Harcanmamış çıktı (coin parçası)	Adres bakiyesi
Fon takibi	Parça bazında, yüksek berraklık	Bakiye bazında, karışım riski
Kümeleme sezgiseli	Ortak girdi sahipliği (CIOH) güçlü	CIOH zayıf; sözleşme analizi gerekir
Akıllı sözleşme	Sınırlı (Script)	Kapsamlı; DeFi, köprü, mixer
Adli zorluk	Düşük–orta	Orta–yüksek (sözleşme etkileşimi)

Not. Kaynak: Nakamoto (2008) ve Meiklejohn ve ark. (2013) temel alınarak derlenmiştir.

burakolgun.com

2.2. Sözde-Anonimlik Yanılgısı

Blokzincir adli analizinin varlık nedeni, kripto varlıkların anonim değil sözde-anonim olmasıdır. Bir adresin arkasındaki gerçek kişi doğrudan görünmez; ancak adres, dünyanın her yerinden erişilebilen kalıcı bir defterde açıkça yer alır. Bu, iki tür bağın kurulmasına olanak tanır. Birincisi, **zincir-içi (on-chain) bağlar**: Adresler arasındaki işlem ilişkileri, ortak harcama örüntüleri ve zamanlama izleri. İkincisi, **zincir-dışı (off-chain) bağlar**: Bir adresin bir borsa hesabına, bir IP adresine, bir KYC (Know Your Customer — müşterini tanı) kaydına veya kamuya açık bir foruma bağlanması. Adli takibin nihai gücü, bu iki katmanı birleştirebilme kapasitesindedir.

Sözde-anonimliğin çözülmesindeki en kritik nokta, çoğu kullanıcının er ya da geç bir **merkezî hizmet** (borsa, ödeme sağlayıcı, ATM) ile temas etmesidir. Suç gelirini nihai olarak harcanabilir bir para birimine (fiat) çevirmek isteyen fail, düzenlemeye tabi bir kripto varlık hizmet sağlayıcısında KYC prosedüründen geçmek zorunda kalır. İşte bu **çıkış noktası** (off-ramp), adli açıdan zincirin en zayıf halkasıdır: On-chain iz, bu noktada gerçek bir kimlikle buluşur. Bu nedenle deneyimli analistler, iz sürmeyi yalnızca 'fonun nereye gittiğini' değil, 'fonun hangi düzenlenmiş kapıdan sisteme girip çıktığını' belirlemeye odaklar.

2.3. Hash Zinciri, Değiştirilemezlik ve Delil Bütünlüğü

Blokzincirin adli değerinin temelinde, blokları birbirine bağlayan kriptografik özet (hash) zinciri yatar. Her blok, kendi işlemlerinin bir özetini (Merkle kökü) ve bir önceki bloğun özetini içerir; bu yapı, defterin geçmişini adeta mühürlenmiş bir zincir hâline getirir. Bir işlem deftere yazıldıktan ve üzerine yeterli sayıda blok eklendikten sonra, o işlemin geriye dönük olarak değiştirilmesi, ardışık tüm blokların yeniden hesaplanmasını gerektirir; bu ise dağıtık bir ağda pratikte olanaksızdır. Adli bilişim açısından bu özellik, geleneksel dijital delillerde büyük emek gerektiren 'değiştirilmemişlik' güvencesini, protokolün doğasından gelen bir garanti hâline getirir.

Ancak bu güvence, yalnızca defterin kendisi için geçerlidir; analistin defterden çıkardığı *yorumlar* için değil. Bir işlem özetinin (transaction hash) değişmezliği tartışmasızken, 'bu adres şu kişiye aittir' biçimindeki bir etiketleme çıkarımı tamamen analistin yöntemine ve veri kaynağına bağlıdır. Bu ayrım, bilirkişilik açısından hayati önemdedir: Defterin ham verisi objektif ve doğrulanabilirken, o veriden türetilen atıf ve kümeleme sonuçları olasılıksaldır ve savunulabilir bir metodolojiyle desteklenmelidir. İyi bir rapor, bu iki katmanı -- değişmez ham veri ile yoruma dayalı çıkarım -- birbirinden özenle ayırır.

3. On-Chain Analiz Metodolojisi

On-chain analiz, açık defterdeki ham veriyi anlamlı, aktörlere bağlı bir istihbarata dönüştüren yöntemler bütünüdür. Bu süreç genellikle beş aşamada ilerler: veri toplama, kümeleme, etiketleme (attribution), iz sürme (tracing) ve görselleştirme. Şekil 1, tipik bir adli takip iş akışını göstermektedir.

burakcinar.com



Kaynak: Chainalysis ve TRM Labs metodolojileri temel alinarak derlenmistir.

Şekil 1. On-Chain Adli Takip İş Akışı (2025)

3.1. Veri Toplama ve Defter Erişimi

Her adli analizin ilk adımı, güvenilir ve eksiksiz veriye erişmektir. Blokzincir verisine erişimin iki temel yolu vardır. Birincisi, analistin kendi çalıştırdığı bir tam düğüm (full node) aracılığıyla defterin doğrudan bir kopyasını tutması ve işlemleri kaynağından doğrulamasıdır; bu yöntem en yüksek güveni ve bağımsızlığı sağlar, çünkü hiçbir üçüncü tarafa güvenmeyi gerektirmez. İkincisi, üçüncü taraf veri sağlayıcıların ve analiz platformlarının sunduğu hazır arayüzlerden yararlanmaktır; bu yöntem daha hızlı ve pratiktir, ancak sağlayıcının veri bütünlüğüne örtük bir güven içerir. İnceleyen ve raporlayan bağlamında, kritik bulguların mümkün olduğunca kaynağından -- bağımsız bir düğüm veya birden çok sağlayıcının karşılaştırılması yoluyla -- doğrulanması, raporun sağlamlığını artırır.

Veri toplama aşamasında dikkat edilmesi gereken bir diğer husus, incelenen olgunun kesin zamansal ve yapısal sınırlarının belirlenmesidir. Hangi blok aralığının, hangi adreslerin ve hangi işlemlerin inceleme kapsamında olduğu, analizin başında açıkça tanımlanmalıdır. Bu kapsam tanımı hem incelemenin yeniden üretilebilirliğini sağlar hem de sonradan 'kapsam kayması' (analizin gerekçesiz biçimde genişlemesi) riskini önler. İyi uygulama, her bulgunun dayandığı işlem özetini (transaction hash) ve blok yüksekliğini kayıt altına almayı gerektirir; böylece bağımsız bir uzman, aynı verilerle aynı sonuca ulaşabilir.

3.2. Kümeleme ve Ortak Girdi Sahipliği Sezgiseli

Kümeleme (clustering), farklı adreslerin aynı gerçek dünya aktörüne (kişi, borsa, servis) ait olduğunu çıkarsayan tekniktir. En güçlü ve en yaygın kümeleme yöntemi, **Ortak Girdi Sahipliği Sezgiseli** (Common Input Ownership Heuristic — CIOH) olarak bilinir. Bu sezgiselin mantığı sadedir: Bir işlemde birden fazla adres girdi olarak kullanılıyorsa, bu

adreslerin tümünü kontrol eden tek bir tarafın olması muhtemeldir; çünkü işlemin geçerli olması için her girdinin özel anahtarıyla imzalanması gerekir. Bu sayede yüzlerce adres, tek bir cüzdan kümesi altında birleştirilebilir. CIOH özellikle UTXO tabanlı Bitcoin'de son derece etkilidir; ancak CoinJoin gibi kasıtlı olarak birden çok kullanıcının girdilerini birleştiren işlemler, bu sezgiseli yanıltmak için tasarlanmıştır.

İkinci önemli sezgisel, **para üstü tespiti** (change detection) olarak adlandırılır. Bir işlemde gönderilen tutar, girdilerin toplamından küçükse, aradaki fark genellikle göndericiye ait yeni bir 'para üstü adresine' geri döner. Analist, hangi çıktının para üstü olduğunu belirleyerek cüzdan kümesini genişletebilir. Bu çıkarımlar olasılıksaldır; yanlış pozitif riski taşır ve bu nedenle inceleme raporunda her sezgiselin dayandığı varsayım ve hata payı açıkça belirtilmelidir. Kümeleme yöntemlerinin performansı, kullanılan sezgisele göre değişir; Tablo 2, tipik karıştırıcı tespit yöntemlerinin ölçülen başarımını özetlemektedir.

Tablo 2. Karıştırıcı (Mixer) Tespit Yöntemlerinin Karşılaştırmalı Başarımı

Yöntem	Kesinlik (Precision)	Duyarlılık (Recall)	Uygulama Notu
Makine öğrenmesi tabanlı	%93	%89	Özellik zengin; etiketli veri gerektirir
Ortak girdi (CIOH)	%88	%79	UTXO'da güçlü; CoinJoin'de zayıflar
Eşit tutar eşleştirme	%82	%75	Basit; yüksek yanlış pozitif riski

Not. Kaynak: karşılaştırmalı akademik ölçümler temel alınarak derlenmiştir. Değerler veri kümesine göre değişkenlik gösterebilir.

3.3. Etiketleme ve Grafik Tabanlı İz Sürme

Kümeleme, adresleri anonim öbeklere ayırır; ancak bu öbeklerin kime ait olduğunu söylemez. Bu boşluğu **etiketleme** (attribution) doldurur. Etiketleme, bir adres kümesini bilinen bir varlığa -- bir borsaya, bir karıştırıcıya, bir fidye yazılımı grubuna, bir yaptırım listesindeki cüzdana -- bağlama sürecidir. Etiket kaynakları çeşitlidir: Borsalardan hukuki süreçle alınan veriler, kamuya açık forum ve sosyal medya paylaşımları, karanlık ağ pazaryerlerinden toplanan istihbarat, honeypot işlemleri ve kolluk iş birlikleri. Ticari analiz platformları (Chainalysis, TRM Labs, Elliptic), milyarlarca etiketlenmiş adresten oluşan devasa veri tabanları üzerine kuruludur ve bir adli analistin tek başına erişemeyeceği bu kolektif istihbarat, iz sürmenin belkemiğini oluşturur.

Etiketlenmiş kümeler üzerinde yürütülen **grafik analizi**, fonların bir aktörden diğerine akışını modelleyerek görselleştirir. Her adres bir düğüm (node), her işlem bir kenar (edge) olarak temsil edilir ve fon akışı bu grafik üzerinde ileri (fonun nereye gittiği) veya geri (fonun nereden geldiği) yönde izlenir. İz sürme sırasında analist, bir 'kirli' kaynaktan başlayıp fonun geçtiği tüm ara durakları -- borsalar, köprüler, karıştırıcılar -- haritalandırır ve nihai çıkış noktasına ulaşmaya çalışır. Bu görselleştirmeler, hem soruşturma ekibinin durumu kavraması hem de mahkeme önünde karmaşık akışın anlaşılır biçimde sunulması açısından paha biçilmezdir; nitekim iyi bir adli rapor, teknik doğruluğu görsel sadelikle birleştirmelidir.

burakolgun.com

Tablo 3. Başlıca Blokzincir Adli Analiz Platformlarının Karşılaştırması

Platform	Öne Çıkan Yön	Tipik Kullanıcı
Chainalysis (Reactor/KYT)	Geniş etiket veri tabanı, uyum entegrasyonu	Kolluk, borsa uyum birimi
TRM Labs	Zincirler arası izleme, yaptırım taraması	Kolluk, düzenleyici kurum
Elliptic	Risk skorlama, DeFi kapsamı	Finansal kuruluş, uyum
Açık kaynak (ör. GraphSense)	Şeffaf, denetlenebilir yöntem	Akademi, bilirkişi

Not. Kaynak: platform kamuya açık dokümantasyonları temel alınarak derlenmiştir. Karşılaştırma tanıtım amacı taşımaz.

3.4. Davranışsal ve Zamansal Sezgiseller

Yapısal sezgisellerin (CIOH, para üstü) ötesinde, modern adli analiz, aktörlerin davranışsal ve zamansal izlerinden de yararlanır. Kullanıcılar, farkında olmadan kendilerine özgü örüntüler bırakır: işlem yapılan saat dilimleri, tercih edilen ücret (fee) düzeyleri, belirli cüzdan yazılımlarının ürettiği karakteristik işlem yapıları ve adres yeniden kullanımı alışkanlıkları. Örneğin, işlemlerin yoğunlaştığı saatler bir coğrafi zaman dilimine işaret edebilir; belirli bir cüzdan istemcisinin girdi sıralama biçimi, kümeleri birbirinden ayırt etmede kullanılabilir. Bu **davranışsal parmak izleri**, tek başına kesin sonuç vermese de, diğer sinyallerle birleştiğinde atıf gücünü artırır.

Zamansal analiz ayrıca, karıştırıcı ve köprü gibi gizleme katmanlarının aşılmasında kritik rol oynar. Bir karıştırıcıya giren ve kısa süre sonra benzer tutarlarda çıkan fonlar arasında, zamanlama korelasyonu olasılıksal bir bağ kurmaya olanak tanır. Aynı biçimde, zincirler arası bir köprünün bir tarafına giren fon ile diğer tarafında çıkan fon, zaman ve tutar örtüşmesiyle eşleştirilebilir. Bu tür korelasyon analizleri, kesin kanıt değil güçlü gösterge üretir; bu nedenle inceleme yaparak raporlayan kişi, bulguyu 'kesin' değil 'yüksek olasılıklı' biçiminde nitelendirmeli ve dayandığı zamansal veriyi raporunda göstermelidir.

4. Gizleme ve Aklama Teknikleri

Failin amacı, on-chain iz ile gerçek kimliği arasındaki bağı koparmaktır. Bu amaçla geliştirilen teknikler, klasik kara para aklamanın üç aşamalı modeline -- yerleştirme (placement), katmanlama (layering) ve bütünleştirme (integration) -- benzer bir mantıkla çalışır; ancak kriptografik araçlarla güçlendirilmiştir. Bu bölümde başlıca gizleme yöntemleri ve bunların adli karşı-tedbirleri ele alınmaktadır.

4.1. Karıştırıcılar (Mixer / Tumbler)

Karıştırıcı (mixer veya tumbler), çok sayıda kullanıcının fonlarını bir havuzda toplayıp yeniden dağıtarak, giriş ve çıkış adresleri arasındaki bağı bulanıklaştıran hizmetlerdir. Merkezî karıştırıcılar bir operatöre güven gerektirir ve bu operatör bir zayıf halka oluşturur. Buna karşın **merkeziyetsiz karıştırıcılar** akıllı sözleşmelerle çalışır; bunların en bilineni, Ethereum üzerinde çalışan ve sıfır bilgi ispatları (zero-knowledge proofs) kullanan Tornado Cash'tir. Tornado Cash, ABD Hazine Bakanlığı tarafından 2022'de yaptırım listesine alınmış; sonraki yıllarda listelenmenin kapsamı ve hukuki dayanağı yargı önünde tartışılmıştır.

burakolgun.com

Karıştırıcılar teknik olarak izi tamamen silmez; giriş ve çıkış zamanlaması, tutar örüntüleri ve havuz büyüklüğü, olasılıksal eşleştirme için kullanılabilir.

CoinJoin tabanlı cüzdanlar (ör. Wasabi) ise, birden çok kullanıcının işlemini tek bir büyük işlemde birleştirerek CIOH sezgiselini kasıtla yanıltır. Bu tür işlemler, ortak girdi sahipliği varsayımını geçersiz kıldığından, analistin katılımcıları ayrıştırmak için ek sinyallere (tutar analizi, alt-küme toplamları, zaman damgaları) başvurmasını gerektirir. Karıştırıcı sonrası iz sürme, adli analizin en zorlu alanlarından biridir ve genellikle kesin değil olasılıksal sonuçlar üretir; bu belirsizlik, inceleme raporunda dürüstçe ifade edilmelidir.

4.2. Zincirler Arası Köprüler ve Chain-Hopping

İz sürmeyi zorlaştıran ikinci büyük teknik, fonların bir blokzincirden diğerine taşınmasıdır (**chain-hopping**). Zincirler arası köprüler (cross-chain bridges) ve merkeziyetsiz takas protokolleri, fonun Bitcoin'den Ethereum'a, oradan başka bir ağa hızla aktarılmasına olanak tanır. Her geçiş, analistin farklı bir defter yapısıyla ve çoğu zaman farklı bir analiz aracıyla çalışmasını gerektirir; iz, ağlar arasındaki 'dikişlerde' kopabilir. Modern adli platformların en önemli gelişmelerinden biri, tam da bu **zincirler arası izleme** yeteneğidir: Bir köprü sözleşmesine giren fon ile diğer tarafta çıkan fonu, zamanlama ve tutar korelasyonuyla eşleştirmek. Bu yetenek olmadan, chain-hopping etkili bir gizleme katmanı olarak kalır.

4.3. Gizlilik Odaklı Coin'ler

Bitcoin ve Ethereum'un açık defterinin aksine, bazı kripto varlıklar gizliliği protokol düzeyinde tasarımlarına gömer. Monero, halka imzalar (ring signatures), gizli adresler (stealth addresses) ve gizli işlem tutarları (RingCT) kullanarak gönderici, alıcı ve tutarı varsayılan olarak gizler; bu, on-chain analizi büyük ölçüde işlevsiz bırakır. Zcash ise sıfır bilgi ispatlarına dayalı 'korumalı' (shielded) işlemler sunar, ancak kullanıcıların çoğunun şeffaf işlem tercih etmesi adli açıdan fırsat yaratır. Bu tür **gizlilik coin'leri**, adli takibin sınırlarını oluşturur; bu durumlarda soruşturma, on-chain veriden çok zincir-dışı delillere (ele geçirilen cihaz, borsa kayıtları, operasyonel hatalar) dayanmak zorunda kalır.

4.4. Katmanlama ve Peel Chain

Failler, tek bir teknikle yetinmez; birden çok yöntemi ardışık katmanlar hâlinde birleştirir. **Peel chain** (soyma zinciri) olarak bilinen örüntüde, büyük bir tutar, her adımda küçük bir parçası 'soyularak' bir dizi ardışık adresten geçirilir; ana kütle ilerlerken küçük parçalar borsalara dağıtılır. Bu, hem tutarı bölerek dikkat çekmemeyi hem de izi uzatarak analisti yormayı amaçlar. Katmanlama, karıştırıcı, köprü ve peel chain'in bir arada kullanıldığı karmaşık senaryolarda en üst düzeye çıkar. Yine de bu tekniklerin hiçbiri defterin değiştirilemezliğini ortadan kaldırmaz; yeterli kaynak, doğru araç ve zincir-dışı veriyle, katmanların önemli bölümü çözülebilir. Bir sonraki bölümdeki Bybit vakası, hem bu tekniklerin sofistike kullanımını hem de adli takibin ulaştığı sınırları somutlaştırmaktadır.

4.5. DeFi, NFT ve Zincir-İçi Yeni Aklama Yüzeyleri

Merkeziyetsiz finans (Decentralized Finance — DeFi) ekosisteminin büyümesi, aklama için yeni yüzeyler açmıştır. Merkeziyetsiz borsalar (DEX), likidite havuzları, borç verme

burakgun.com

protokolleri ve otomatik piyasa yapıcılar, fonların bir varlıktan diğerine hızla ve bir aracıya kimlik vermeden dönüştürülmesine olanak tanır. Fail, çalınan bir varlığı birkaç protokol üzerinden farklı token'lara çevirerek izi bulanıklaştırabilir. Benzer biçimde, değeri öznel olan ve kolayca şişirilebilen dijital varlıklar -- örneğin NFT'ler -- 'öz ticaret' (wash trading) yoluyla değer aktarımının gizlenmesinde kullanılabilir. Bu yeni yüzeyler, adli analistin yalnızca basit transferleri değil, akıllı sözleşme etkileşimlerini de çözümleyebilmesini gerektirir.

Ne var ki DeFi'nin şeffaflığı, aynı zamanda bir adli fırsattır. Merkeziyetsiz protokollerin çoğu, işlemlerini açık defterde ve denetlenebilir akıllı sözleşmeler aracılığıyla gerçekleştirir; bu da her etkileşimin -- takas, havuza giriş, borç alma -- kalıcı iz bıraktığı anlamına gelir. Merkezî bir aracının kaçınılmaz olarak kimlik topladığı klasik sistemin aksine, DeFi kimlik toplamasa da her adımı kaydeder. Bu nedenle deneyimli bir analist için DeFi, izi kaybetmek yerine, akıllı sözleşme mantığını doğru okuduğunda izi sürdürebileceği zengin bir veri kaynağıdır. Belirleyici olan, aracın ve analistin sözleşme düzeyindeki etkileşimleri çözümleyebilme kapasitesidir.

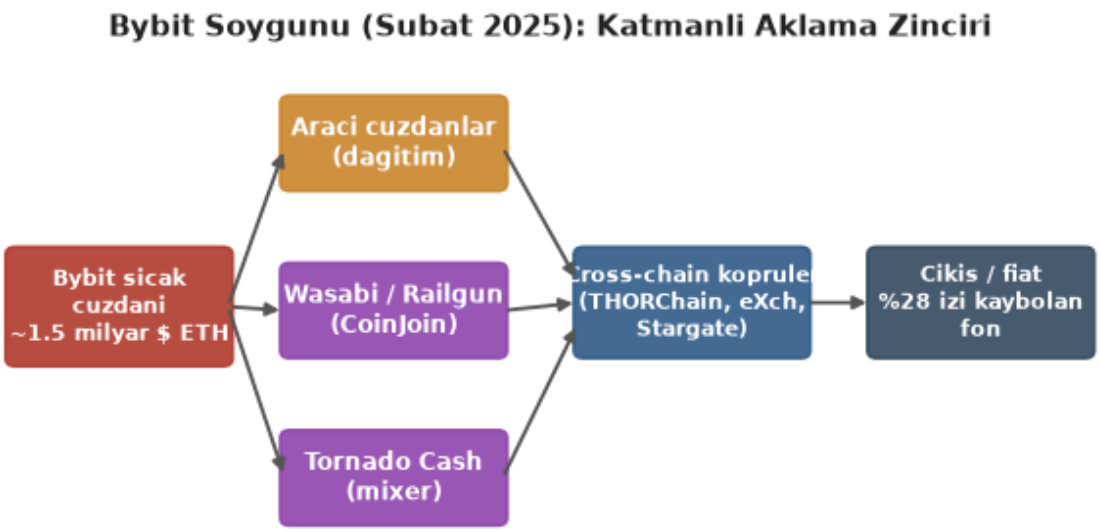
5. Vaka İncelemesi: Bybit Soygunu (Şubat 2025)

21 Şubat 2025 tarihinde, merkezi Dubai'de bulunan Bybit kripto para borsası, yaklaşık 1,5 milyar dolar değerinde Ethereum'un (ETH) çalınmasıyla kripto tarihinin en büyük tekil dijital soygununa maruz kaldı. ABD Federal Soruşturma Bürosu (FBI), 26 Şubat 2025'te olayı Kuzey Kore bağlantılı Lazarus grubuna resmen atfetti (FBI, 2025). Bu vaka, hem saldırının teknik yöntemi hem de sonrasındaki aklama zinciri açısından, modern blokzincir adli analizinin hem gücünü hem de sınırlarını örnekleyen bir laboratuvar niteliğindedir.

Saldırının kökeni, doğrudan blokzincirde değil, insan ve tedarik zinciri katmanındaydı. Raporlara göre bir geliştirici (DevOps) mühendisine, LinkedIn üzerinden sahte bir iş teklifi kisvesinde zararlı yazılım içeren bir dosya ulaştırıldı; bu yolla saldırganlar, Bybit'in kullandığı çoklu imza cüzdan altyapısı Safe{Wallet}'ın geliştirme ortamına sızdı. 19 Şubat'taki rutin bir güncelleme sırasında imza arayüzüne kötü niyetli kod enjekte edildi; böylece imzayı onaylayan yetkililer meşru bir işlemi onayladıklarını sanırken, gerçekte fonların saldırgan kontrolündeki adreslere aktarılmasına izin veren bir işlemi imzaladılar. Fonlar yaklaşık 23 dakika içinde boşaltıldı. Bu ayrıntı, adli açıdan önemli bir dersi vurgular: On-chain iz sürme ne kadar güçlü olursa olsun, ihlalin kök nedeni çoğu zaman zincir-dışı bir sosyal mühendislik veya tedarik zinciri saldırısıdır.

Çalınan fonun aklanması, dördüncü bölümde anlatılan tekniklerin adeta bir vitrinidir. Saldırganlar önce fonları çok sayıda aracı cüzdana dağıttı; ardından Tornado Cash, Wasabi Wallet, Railgun ve çeşitli karıştırıcılardan geçirdi; nihayet THORChain, eXch, Lombard, LiFi, Stargate ve SunSwap gibi zincirler arası takas ve köprü protokolleriyle fonları ağdan ağa taşıdı (TRM Labs, 2025). Şekil 3, bu katmanlı aklama zincirinin sadeleştirilmiş bir şemasını sunmaktadır. Blokzincir istihbarat şirketleri, fonların önemli bir bölümünü gerçek zamanlı olarak izleyerek borsaları uyardı ve bazı varlıkların dondurulmasını sağladı; ancak raporlara göre çalınan tutarın yaklaşık %28'i, katmanlı gizleme nedeniyle izlenemez hâle geldi.

burakolgun.com



Şekil 3. Bybit Soygununda Katmanlı Aklama Zinciri (2025)

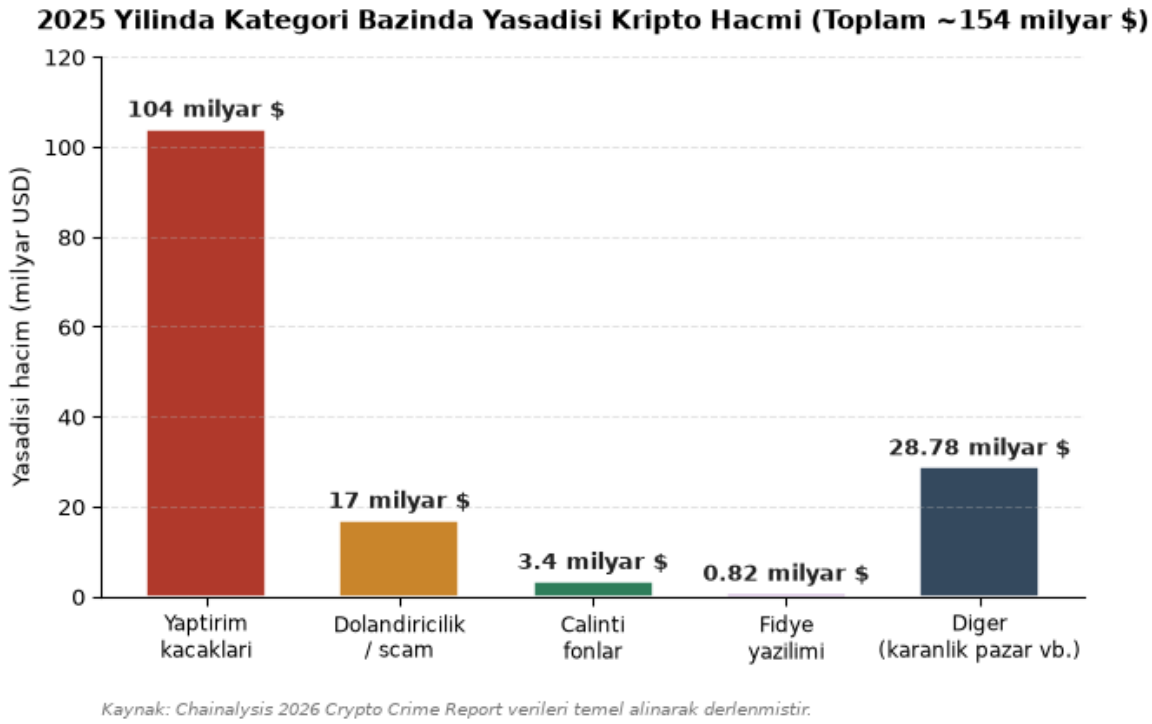
Vakanın atıf boyutu da öğreticidir. Kuzey Kore bağlantılı grupların kripto soygunlarında kullandığı altyapı, aklama örüntüleri ve tekrar eden operasyonel alışkanlıklar, yıllar içinde blokzincir analistleri tarafından ayrıntılı biçimde belgelenmiştir. Bybit olayında da atıf, tek bir işleme değil; kullanılan cüzdan kümelerinin önceki saldırılarla kesişmesine, aklama yönteminin karakteristik imzasına ve bağımsız istihbarat kaynaklarının örtüşmesine dayandırılmıştır. Bu, adli atfın en sağlam biçiminin, çok sayıda bağımsız delil katmanının aynı sonuca işaret etmesiyle kurulduğunu gösterir. FBI'ın kamuoyu duyurusu ve blokzincir istihbarat şirketlerinin bağımsız analizleri, birbirini bu şekilde teyit ederek atfın güvenilirliğini pekiştirmiştir.

Bybit vakasından çıkarılacak adli dersler çok katmanlıdır. Birincisi, blokzincir adli analizi, saldırıyı önlemese de, saldırı sonrasında failin izini gerçek zamanlı sürerek aklamanın önemli bölümünü engelleyebilir; bu, geleneksel finansta neredeyse imkânsız bir hızdır. İkincisi, gizleme teknikleri iyi kaynaklı bir devlet destekli aktör tarafından katmanlı biçimde kullanıldığında, fonun bir kısmı kalıcı olarak izlenemez hâle gelebilir; yani on-chain analiz güçlü ama mutlak değildir. Üçüncüsü, atıf (attribution) süreci -- olayı belirli bir aktöre bağlamak -- yalnızca on-chain örüntülere değil, aynı zamanda önceki saldırılarla kesişen adres kümelerine, kullanılan altyapıya ve istihbarat iş birliğine dayanır. Bu bütüncül yaklaşım, bir inceleme yaparak raporlayan kişinin de benimsemesi gereken yöntemsel duruştur.

6. Yasadışı Kripto Ekonomisinin 2025 Görünümü

Bireysel vakaların ötesinde, yasadışı kripto ekonomisinin bütünsel görünümü, adli önceliklerin belirlenmesi açısından yol göstericidir. Chainalysis'in 2026 raporuna göre 2025 yılında yasadışı adreslerin aldığı toplam değer en az 154 milyar dolara ulaşmıştır; bu, revize edilmiş 2024 rakamı olan yaklaşık 57,2 milyar dolara kıyasla çarpıcı bir artıştır (Chainalysis, 2026). Şekil 2, bu hacmin başlıca kategorilere dağılımını göstermektedir.

burakolgun.com



Şekil 2. 2025 Yılında Kategori Bazında Yasadışı Kripto Hacmi (2025)

Verinin en dikkat çekici yönü, artışın büyük ölçüde **yaptırım kaçakçılığından** kaynaklanmasıdır: Yaptırım kapsamındaki aktörlerin aldığı değer, yıllık bazda yaklaşık %694 artarak yaklaşık 104 milyar dolara ulaşmıştır. Bunu tahmini 17 milyar dolarlık dolandırıcılık ve scam faaliyetleri, hack yoluyla çalınan yaklaşık 3,4 milyar dolarlık fon ve yaklaşık 820 milyon dolarlık fidye yazılımı ödemeleri izlemektedir. Ayrıca, yaptırım listesindeki aktörlerle ilişkili devlet destekli grupların -- özellikle Kuzey Kore bağlantılı Lazarus'un -- 2025 yılında yaklaşık 2 milyar dolar çaldığı belirtilmektedir. Bu tablo, kripto suçunun artık bireysel dolandırıcılıktan çok, jeopolitik ölçekli ve devlet destekli bir boyut kazandığını göstermektedir.

Bir diğer yapısal dönüşüm, sabit-değerli kripto varlıkların (stablecoin) yasadışı hacimdeki payının %84'e ulaşmasıdır. Failler, oynaklığı yüksek Bitcoin yerine, değerini koruyan stablecoin'leri tercih etmektedir; ancak bu tercih, adli açıdan bir fırsat da barındırır: Başlıca stablecoin ihraççıları merkezîdir ve hukuki talep üzerine belirli adresleri dondurabilir. Nitekim 2025'te bu dondurma mekanizması, çalınan fonların bir bölümünün kurtarılmasında etkili olmuştur. Bu, adli stratejinin yalnızca teknik iz sürmeyle değil, ihraççılar ve borsalarla kurulan hukuki iş birliğiyle de yürütülmesi gerektiğini göstermektedir.

Tablo 4. Başlıca Yasadışı Kategoriler ve Adli Yaklaşım Başlangıç Noktaları

Kategori	Adli Başlangıç Noktası	Öncelikli Yöntem
Fidye yazılımı	Fidye ödeme adresi	Ödemeden geriye küme çıkarımı
Borsa/protokol hack'i	Çalınan fon çıkış işlemi	Gerçek zamanlı iz sürme + dondurma
Yatırım dolandırıcılığı	Mağdur ödeme adresleri	Toplama cüzdanı ve off-ramp tespiti

burakolgun.

Karanlık pazar	Pazaryeri emanet (escrow) adresi	Ödeme akışı ve kullanıcı kümeleme
Yaptırım kaçakçılığı	Listelenmiş cüzdan teması	Yaptırım taraması + zincirler arası izleme

Not. Kaynak: Chainalysis (2026) ve Europol (2024) tipolojileri temel alınarak derlenmiştir.

Fidye yazılımı (ransomware) ekonomisi, kripto adli analizinin en olgun uygulama alanlarından biridir. Fidye ödemeleri neredeyse tümüyle kripto varlıkla yapıldığından, ödeme adresleri soruşturmanın başlangıç noktasını oluşturur; bu adreslerden yola çıkarak ödemeyi alan grubun cüzdan kümesi, kullandığı karıştırıcılar ve nihai çıkış noktaları haritalandırılabilir. 2025 verilerine göre fidye ödemeleri yaklaşık 820 milyon dolar düzeyinde gerçekleşmiştir; ancak asıl önem, bu ödemelerin izlenerek fidye ekosisteminin altyapısının deşifre edilmesindedir. Blokzincir analizi, bir fidye kampanyasının arkasındaki 'hizmet olarak fidye yazılımı' (ransomware-as-a-service) modelini, bağlı aktörler (affiliate) arasındaki kâr paylaşımını ve grubun operasyonel altyapısını ortaya çıkarabilir.

Karanlık ağ (darknet) pazaryerleri de kripto adli analizinin sürekli hedeflerindendir. Bu pazaryerleri uyuşturucu, çalıntı veri ve yasadışı hizmetlerin kripto varlıkla alınıp satıldığı platformlardır; ödeme akışlarının izlenmesi, hem pazaryeri operatörlerinin hem de yoğun kullanıcıların tespitine olanak tanır. Tarihsel olarak, en büyük karanlık ağ operasyonlarının çökertilmesinde blokzincir iz sürme belirleyici rol oynamıştır. Bu deneyimler, ortak bir dersi pekiştirir: Suçlular anonimlik varsayımıyla hareket ederken, defterin kalıcı hafızası, çoğu zaman yıllar sonra bile izin sürülmesine olanak tanımaktadır. Kripto suçunun caydırıcılığı, tam da bu gecikmeli ama kalıcı izlenebilirlikten beslenmektedir.

7. Delil Zinciri ve Adli Bilişim Süreci

On-chain analizin ürettiği bulguların soruşturma dosyasında ve mahkemede kullanılabilmesi, adli bilişimin temel ilkelerine uygun bir sürecin izlenmesine bağlıdır. Teknik doğruluk gerekli ama yeterli değildir; bulgunun hukuka uygun toplanmış, bütünlüğü korunmuş ve yeniden üretilebilir olması gerekir.

7.1. El Koyma ve Cüzdanın Ele Geçirilmesi

Kripto varlıklara el koyma, geleneksel el koymadan farklı teknik gerektirir. Varlığın kontrolü, fiziksel bir nesnede değil, **özel anahtarda** (private key) veya bunu türeten **kurtarma tohumunda** (seed phrase) yatar. Bu nedenle bir cihaza (bilgisayar, telefon, donanım cüzdanı) el konulduğunda, adli ekibin öncelikli hedefi, varlığı kolluk kontrolündeki güvenli bir cüzdana taşımak için gereken anahtar materyaline hukuka uygun biçimde ulaşmaktır. Anahtar ele geçirilemezse, varlığın varlığı tespit edilse bile ona el konulamaz; bu, geleneksel el koymadan temel bir farktır. El koyma anında cüzdanın durumunun (bakiye, adres listesi, işlem geçmişi) titizlikle belgelenmesi, sonraki analiz için kritiktir.

7.2. Delil Bütünlüğü ve Chain of Custody

Adli sürecin kalbinde **delil zinciri** (chain of custody) ve **bütünlük** (integrity) kavramları yer alır. On-chain veri, kamuya açık ve değiştirilemez olsa da, analistin bu veriden hangi çıkarımları hangi yöntemle yaptığı belgelenmelidir. İyi uygulama, incelenen işlem ve

burakolgun.com

blokların blok yüksekliği (block height) ve işlem özeti (transaction hash) ile kesin biçimde tanımlanmasını, kullanılan araç ve sürümlerinin kaydedilmesini ve analizin bağımsız bir uzman tarafından aynı verilerle yeniden üretilebilmesini gerektirir. Ele geçirilen dijital delillerin (cüzdan dosyaları, cihaz imajları) kriptografik özeti (hash) alınmalı ve el koyma anından itibaren her aktarım kayıt altına alınmalıdır. Bu titizlik, raporun mahkemede sorgulanması hâlinde teknik bulgunun ayakta kalmasını sağlar.

7.3. Raporlama

Bir blokzincir adli raporu, üç okuyucu kitlesini aynı anda tatmin etmelidir: teknik uzman, hukukçu ve hâkim. Bu nedenle rapor, hem yöntemin teknik olarak savunulabilir olmasını hem de teknik olmayan okuyucu için anlaşılır kalmasını dengelemelidir. İyi bir rapor, her iddiayı belirli bir işlem özetine bağlar; olasılıksal çıkarımların (kümeleme, para üstü tespiti) belirsizliğini açıkça belirtir; ve etiketleme kaynaklarının güvenilirliğini tartışır. Raporu yazan kişi, ticari bir analiz aracının verdiği sonucu sorgusuz aktarmak yerine, aracın dayandığı sezgiselleri ve olası hata kaynaklarını anlamalı ve raporda şeffaf biçimde belirtmelidir. Aksi hâlde, teknik olarak doğru görünen ancak metodolojik olarak sorgulanabilir bir rapor, savunma tarafından haklı olarak çürütülebilir.

7.4. Müsadere ve Varlık Geri Kazanımı

Adli sürecin nihai amaçlarından biri, suçtan elde edilen kripto varlığın müsadere edilerek ekonomik kazancın failden geri alınmasıdır. Bu, hem cezalandırıcı hem de caydırıcı bir işlev taşır; zira ekonomik suçun mantığı, kazancın korunabilmesine dayanır. Kripto varlıkların müsaderesinde iki teknik önkoşul öne çıkar: varlığın hukuka uygun biçimde tespit ve tanımlanması (hangi adreste, ne kadar) ve varlığa fiilen el konulabilmesi için gereken anahtar materyaline erişim. Anahtar ele geçirilemediğinde, mahkeme kararı olsa dahi varlık fiilen taşınamayabilir; bu durumda varlık, ilgili adreste 'dondurulmuş' kalır ancak erişilemez.

Varlık geri kazanımında zamanlama kritiktir. Merkezî bir hizmet sağlayıcıya (borsa, stablecoin ihraççısı) ulaşan çalıntı fon, hukuki talep üzerine dondurulabilir; ancak bu fırsat penceresi çoğu zaman saatlerle sınırlıdır. Bu nedenle etkili geri kazanım, gerçek zamanlı iz sürme ile hızlı hukuki müdahalenin eşgüdümünü gerektirir. Uluslararası boyutta, farklı yargı çevrelerindeki varlıkların geri kazanımı, adli yardımlaşma anlaşmalarına ve giderek gelişen uluslararası iş birliği ağlarına dayanır.

7.5. Otomasyon, Yapay Zekâ ve İnsan Denetimi

Blokzincir adli analizinin hacmi ve karmaşıklığı, otomasyonu zorunlu kılmaktadır. Milyonlarca işlemi elle incelemek olanaksız olduğundan, kümeleme, risk skorlama ve örüntü tanıma işlevleri giderek makine öğrenmesi ve yapay zekâ modellerine devredilmektedir. Bu araçlar, insan analistin gözden kaçırabileceği ince örüntüleri saptayabilir ve büyük veri kümelerini saniyeler içinde tarayabilir. Ancak otomasyonun getirdiği hız, beraberinde bir sorumluluk getirir: Bir modelin ürettiği risk skoru ya da küme önerisi, nihai bir gerçek değil, insan uzmanın doğrulaması gereken bir hipotezdir.

Adli bağlamda 'kara kutu' niteliğindeki bir yapay zekâ çıktısının sorgusuz kabul edilmesi, ciddi bir metodolojik risktir; çünkü savunma tarafı, modelin nasıl karar verdiğini

burakolgun.com

haklı olarak sorgulayabilir. Bu nedenle iyi uygulama, otomatik araçların **açıklanabilir** (explainable) sonuçlar üretmesini ve her kritik bulgunun insan uzman tarafından gerekçelendirilmesini gerektirir. Yapay zekâ, adli analistin yerini almaz; onun kapasitesini genişleten, ancak nihai muhakemeyi ve sorumluluğu insana bırakan bir araçtır. Mahkeme önünde sorumlu olan, modeldir değil, raporu imzalayan inceleme yapan kişidir; dolayısıyla inceleme yapan kişi, aracın ürettiği her sonucu anlamak ve savunabilmek zorundadır.

8. Hukuki Çerçeve

Blokzincir adli analizinin çıktıları, ancak uygun bir hukuki çerçeve içinde anlam kazanır. Bu bölüm, konuyu önce Türk hukuku, ardından uluslararası düzenlemeler açısından ele almaktadır.

8.1. Türk Hukuku: 7518 Sayılı Kanun, MASAK ve TCK m. 282

Türkiye'de kripto varlıklara ilişkin en önemli düzenleme, 2 Temmuz 2024 tarihli Resmî Gazete'de yayımlanan **7518 sayılı Kanun**'dur. Bu Kanun, 6362 sayılı Sermaye Piyasası Kanunu'nda değişiklik yaparak kripto varlığı 'dağıtık defter teknolojisi veya benzer bir teknoloji kullanılarak elektronik olarak oluşturulup saklanabilen, dijital ağlar üzerinden dağıtımı yapılan ve değer veya hak ifade edebilen gayri maddi varlıklar' biçiminde tanımlamıştır. Kanun, kripto varlık hizmet sağlayıcılarını (KVHS) Sermaye Piyasası Kurulu (SPK) gözetimine ve lisans rejimine tabi kılmıştır (7518 sayılı Kanun, 2024).

Adli takip açısından en kritik dönüşüm, KVHS'lerin **MASAK** (Mali Suçları Araştırma Kurulu) mevzuatı kapsamında yükümlü kılınması ve bu bağlamda finansal kuruluş statüsüne yaklaştırılmasıdır. Bu statü, KVHS'leri müşterini tanı (KYC), şüpheli işlem bildirimi ve kayıt tutma yükümlülükleri bakımından bankalar ve ödeme kuruluşlarıyla aynı sınıfa taşır. Uygulamada bu, on-chain analizin çıkış noktasında (off-ramp) gerçek kimliğe ulaşmayı kolaylaştıran bir hukuki altyapı yaratır: Bir Türk KVHS'sine giren fonun arkasındaki kişi, hukuki talep üzerine tespit edilebilir hâle gelir.

Ceza hukuku boyutunda, kripto varlıklar aracılığıyla suç gelirlerinin aklanması, **Türk Ceza Kanunu'nun 282. maddesi** kapsamında 'suçtan kaynaklanan malvarlığı değerlerini aklama' suçunu oluşturur. Bu suçun cezası, üç yıldan yedi yıla kadar hapis ve yirmi bin güne kadar adli para cezasıdır. Kripto varlığın araç olarak kullanılması, suçun niteliğini değiştirmez; ancak delillendirme, klasik aklamadan farklı olarak blokzincir adli analizini gerektirir. El koyma, arama ve inceleme işlemleri ise Ceza Muhakemesi Kanunu'nun ilgili hükümlerine (özellikle bilgisayarlarda arama ve el koymaya ilişkin CMK m. 134) uygun biçimde yürütülmelidir; aksi hâlde elde edilen delil hukuka aykırı sayılabilir.

8.2. Uluslararası Düzenlemeler: FATF, MiCA ve Yaptırımlar

Uluslararası düzlemde, Mali Eylem Görev Gücü'nün (Financial Action Task Force — FATF) getirdiği **Seyahat Kuralı** (Travel Rule) belirleyicidir. Bu kural, belirli bir eşiğin üzerindeki kripto transferlerinde, gönderen ve alıcıya ilişkin tanımlayıcı bilgilerin hizmet sağlayıcılar arasında paylaşılmasını gerektirir; böylece kripto transferleri, geleneksel havalelerdeki izlenebilirlik standardına yaklaştırılır (FATF, 2021). Avrupa Birliği'nde ise **MiCA** (Markets in Crypto-Assets) tüzüğü, kripto varlık piyasalarını kapsamlı biçimde

burakolgun.com

düzenleyerek hizmet sağlayıcılara ruhsat ve uyum yükümlülükleri getirmiştir (EU MiCA, 2023). Bu düzenlemeler, on-chain analizin zincir-dışı kimlik verisiyle birleştirilebilmesi için gereken kurumsal altyapıyı güçlendirmektedir.

Yaptırımlar rejimi de giderek merkezî bir rol oynamaktadır. ABD Hazine Bakanlığı'na bağlı OFAC'in (Office of Foreign Assets Control) belirli cüzdan adreslerini ve hatta bir karıştırıcı protokolünü (Tornado Cash) yaptırım listesine alması, kod ve protokollere yaptırım uygulanabilirliği konusunda önemli hukuki tartışmalar başlatmıştır. Adli analist ve bilirkişi açısından bu, bir fonun yalnızca 'suç geliri' olup olmadığını değil, aynı zamanda 'yaptırımlı bir adresle' temas edip etmediğini de değerlendirmesi gerektiği anlamına gelir. Yaptırım taraması, modern blokzincir analiz platformlarının standart bir işlevi hâline gelmiştir.

8.3. Uluslararası İş Birliği ve Atıf Standardı

Kripto varlıkların sınır tanımayan yapısı, adli sürecin de doğası gereği uluslararası olmasını gerektirir. Bir Türk soruşturmasında izi sürülen fon, dakikalar içinde farklı yargı çevrelerindeki borsalara, köprülere ve hizmet sağlayıcılara ulaşabilir. Bu nedenle etkin bir soruşturma, adli yardımlaşma anlaşmalarına (MLAT), doğrudan kolluk iş birliği ağlarına ve giderek gelişen uluslararası kripto varlık geri kazanım mekanizmalarına dayanır. Ancak bu süreçlerin klasik hızı, kripto fonlarının hareket hızıyla kıyaslandığında yavaş kalır; bu asimetri, önceden kurulmuş hızlı bildirim kanallarının ve borsalarla sürdürülen operasyonel iş birliğinin önemini artırır.

Uluslararası boyutun bir diğer kritik yönü, **atıf standardıdır**. Bir saldırıyı ya da fon akışını belirli bir aktöre -- örneğin devlet destekli bir gruba -- bağlamak, yalnızca on-chain örüntülere değil; kullanılan altyapının, önceki olaylarla kesişen adres kümelerinin ve bağımsız istihbarat kaynaklarının bir arada değerlendirilmesine dayanır. Bu bütüncül atıf yaklaşımı, tek bir sinyale dayanan aceleci sonuçların yol açabileceği hataları önler. İnceleme yapan kişi açısından benimsenmesi gereken ilke nettir: Atıf, kesinlik derecesi açıkça belirtilerek ve dayandığı kanıt katmanları şeffaf biçimde gösterilerek yapılmalı; doğrulanmamış bir çıkarım, hiçbir zaman kesin bir tespit gibi sunulmamalıdır.

9. Türkiye Bağlamı ve Uygulama

Türkiye, kripto varlık kullanımının yoğun olduğu ülkelerden biridir; bu durum, hem yasadışı kullanım riskini hem de adli takip ihtiyacını artırmaktadır. 7518 sayılı Kanun'un getirdiği lisans ve MASAK rejimi, yerli borsaların uyum kapasitesini yükseltmiş; bu da yurt içi off-ramp noktalarından kimlik tespitini kolaylaştırmıştır. Ancak failler, yurt dışı borsaları, eşler arası (P2P) işlemleri ve merkeziyetsiz platformları kullanarak bu denetimden kaçmaya çalışmaktadır; bu da uluslararası adli iş birliğini zorunlu kılar.

Uygulamada Türk soruşturma makamları, blokzincir adli analizinde üç tür zorlukla karşılaşır. Birincisi **kapasite**: On-chain analiz, özel araçlar ve eğitimli uzman gerektirir; bu kapasitenin kolluk ve adliye bünyesinde yaygınlaştırılması gerekir. İkincisi **veri erişimi**: Yurt dışı borsalardan veri temini, uluslararası adli yardımlaşma (MLAT) süreçlerine bağlıdır ve zaman alır; oysa kripto fonları dakikalar içinde hareket eder. Üçüncüsü **hukuki nitelendirme**:

burakolgun.com

Kripto varlığın malvarlığı değeri olarak nitelendirilmesi, el koyma ve müsadere işlemlerinin hukuki dayanağı bakımından dikkatli bir yaklaşım gerektirir.

Bu zorluklara karşı önerilebilecek yaklaşım, teknik ve hukuki uzmanlığın bir arada yürütüldüğü, disiplinler arası bir soruşturma modelidir. Inceleme ve raporlama uygulamasında, analistin yalnızca bir ticari aracın çıktısını sunması değil; kullanılan sezgiselleri, etiket kaynaklarını ve belirsizlik paylarını açıkça ortaya koyan, yeniden üretilebilir bir rapor hazırlaması beklenmelidir. Ayrıca, yurt içi KVHS'lerle kurulacak hızlı ve hukuka uygun veri paylaşımı kanalları, fonların dondurulması için kritik olan zaman penceresini değerlendirme açısından belirleyicidir.

Türkiye'nin bir diğer yapısal avantajı, kripto varlık kullanımının yaygınlığı sayesinde oluşan büyük yerli hizmet sağlayıcı ekosistemidir. Bu ekosistem, 7518 sayılı Kanun'un getirdiği uyum yükümlülükleriyle birlikte, yurt içinde gerçekleşen off-ramp işlemlerinin önemli bölümünün kayıt altında olması anlamına gelir. Etkin bir soruşturma modeli, bu yerli kayıtları -- KYC verileri, şüpheli işlem bildirimleri, işlem günlükleri -- on-chain iz sürmeyle birleştirdiğinde, failin gerçek kimliğine ulaşma olasılığı belirgin biçimde artar. Kritik olan, bu iki veri katmanı arasındaki köprünün hukuka uygun ve hızlı biçimde kurulabilmesidir.

Eğitim ve kapasite geliştirme, Türkiye bağlamının en acil ihtiyacıdır. Blokzincir adli analizi, hem teknik derinlik hem de hukuki muhakeme gerektiren melez bir uzmanlıktır; bu uzmanlığın hâkim, savcı ve kolluk düzeyinde yaygınlaştırılması, adaletin kalitesini doğrudan etkiler. Bilirkişilik kurumunun bu alanda güçlendirilmesi -- alanında yetkin, metodolojik olarak şeffaf ve bağımsız inceleme yapan bilirkişilerin yetiştirilmesi -- hem yanlış atıf riskini azaltır hem de teknik bulguların mahkemede hak ettiği ağırlığı kazanmasını sağlar. Nitekim bir adli raporun değeri, kullandığı aracın gücünden çok, o aracı kullanan uzmanın yöntemsel titizliğiyle ölçülür. Ancak diğer taraftan günümüz uygulamasında bilirkişilik mekanizmasının içerisinde ticari amaç güden firmalara kurumsal bilirkişi olarak yer verilmesi de ticari kaygıyı ön plana çıkartması nedeniyle bağımsızlık ilkesine gölge düşürmektedir.

9.1. Temsilî Bir Soruşturma Senaryosu

Kavramların somutlaşması için, gerçek bir dosyaya atıf yapmayan, tümüyle temsilî bir senaryo düşünelim. Bir yatırım dolandırıcılığı mağduru, kendisine ait bir miktar stablecoin'i, yüksek getiri vaadiyle bir cüzdana gönderdiğini ve sonrasında erişimini kaybettiğini beyan etmiştir. Soruşturmanın başlangıç noktası, mağdurun ödeme yaptığı hedef adrestir. Analist önce bu adresi ve onunla ortak girdi paylaşan adresleri kümeleyerek failin toplama cüzdanını belirler; ardından bu kümeye giren diğer mağdur ödemelerini tespit ederek dolandırıcılığın gerçek ölçeğini ortaya çıkarır.

İkinci aşamada analist, toplanan fonun nasıl aklandığını izler. Fonun bir bölümünün bir karıştırıcıya, bir bölümünün ise zincirler arası bir köprüyle başka bir ağa aktarıldığı görülür. Karıştırıcı sonrası iz olasılıksal hâle gelirken, köprü üzerinden geçen fon, zamanlama ve tutar korelasyonuyla diğer ağda yeniden yakalanır. Nihayet fonun bir kısmının, düzenlemeye tabi bir borsanın yatırma adresine ulaştığı saptanır. İşte bu **çıkış noktası**, soruşturmanın kilit halkasıdır: Borsaya yöneltilecek hukuka uygun bir talep, o yatırma adresinin arkasındaki KYC kaydını -- yani gerçek kimliği -- açığa çıkarabilir.

burakolgun.com

Üçüncü aşamada, tüm bu bulgular bir adli raporda birleştirilir. Rapor, her adımı ilgili işlem özetiyle belgelendirir; kümeleme ve para üstü çıkarımlarının olasılıksal doğasını açıkça belirtir; karıştırıcı sonrası izin belirsizlik payını dürüstçe ifade eder; ve borsa kaydıyla kurulan zincir-dışı bağı, off-chain delil olarak ayrı biçimde niteler. Bu senaryo, makalenin ana tezini örneklemektedir: On-chain analiz güçlü bir başlangıç sağlar, ancak sonuç ancak zincir-dışı kimlik verisiyle birleştiğinde ve delil zinciri korunduğunda mahkeme önünde tam değerine ulaşır. Vurgulamak gerekir ki bu senaryo tümüyle açıklayıcı amaçlıdır ve herhangi bir gerçek dosya veya kişiyle ilişkili değildir.

10. Zorluklar, Sınırlar ve Öneriler

Blokzincir adli analizi güçlü bir disiplindir; ancak sınırları dürüstçe kabul edilmelidir. Aşağıdaki maddeler, alanın başlıca zorluklarını ve bunlara ilişkin önerileri özetlemektedir:

- **Olasılıksal çıkarım:** Kümeleme ve para üstü tespiti gibi sezgiseller kesin değil olasılıksaldır; raporda hata payı ve varsayımlar açıkça belirtilmelidir.
- **Gizlilik coin'leri:** Monero gibi protokol düzeyinde gizli ağlarda on-chain analiz büyük ölçüde işlevsizdir; bu durumlarda zincir-dışı delillere yönelmek gerekir.
- **Zincirler arası kaçış:** Chain-hopping, izi ağlar arasında koparabilir; zincirler arası izleme yeteneği olmayan araçlar yetersiz kalır.
- **Atıf riski:** Bir kümeyi belirli bir kişiye bağlamak, zincir-dışı doğrulama olmadan spekülatif kalır; yanlış atıf ciddi bir adli hata kaynağıdır.
- **Hız asimetrisi:** Fonlar dakikalar içinde hareket ederken, hukuki talep süreçleri günler alır; hızlı müdahale için borsalarla önceden kurulmuş kanallar gerekir.
- **Araç bağımlılığı:** Ticari platformlara körü körüne güven, metodolojik şeffaflığı zayıflatır; mümkün olduğunda denetlenebilir, açık yöntemler tercih edilmelidir.

Bu önerilerin ortak paydası, teknik yetkinliğin hukuki titizlik ve metodolojik şeffaflıkla birleştirilmesidir. On-chain analiz, tek başına bir 'sihirli değnek' değil; ancak zincir-dışı veriyle ve sağlam bir delil zinciriyle birleştirildiğinde, çağdaş ekonomik suçla mücadelenin en etkili araçlarından biridir.

11. Sonuç

Kripto varlıkların sağladığı sözde-anonimlik, uzun süre suç failleri için bir sığınak olarak algılanmıştır. Oysa bu makalede gösterildiği üzere, çoğu blokzincirin açık ve değiştirilemez defter yapısı, geleneksel finansal sistemde erişilmesi güç olan bir izlenebilirlik sunmaktadır. On-chain analiz -- kümeleme, etiketleme ve grafik tabanlı iz sürme yoluyla -- anonim adresleri gerçek dünya aktörlerine bağlayabilmekte; karıştırıcı, köprü ve katmanlama gibi gizleme teknikleri karşısında bile önemli sonuçlar üretebilmektedir.

Bununla birlikte, on-chain analizin gücü mutlak değildir. Bybit vakasının gösterdiği gibi, iyi kaynaklı bir aktör, katmanlı gizlemeyle fonun bir bölümünü kalıcı olarak izlenemez hâle getirebilir; gizlilik coin'leri ise analizin doğal sınırını oluşturur. Bu nedenle blokzincir adli analizi, zincir-dışı kimlik verisiyle -- borsa kayıtları, ele geçirilen cihazlar, operasyonel hatalar -- birleştirildiğinde tam değerine ulaşır. Türkiye açısından 7518 sayılı Kanun ile

burakolgun.com

kurulan lisans ve MASAK rejimi, bu birleşimi mümkün kılan hukuki altyapıyı güçlendirmekte; ancak kapasite, veri erişimi ve hız asimetrisi gibi pratik sorunlar aşılmayı beklemektedir.

Bu makalenin ortaya koyduğu bir diğer örüntü, teknoloji ile düzenleme arasındaki sürekli yarıştır. Her yeni gizleme tekniği -- merkeziyetsiz karıştırıcılar, zincirler arası köprüler, gizlilik coin'leri -- adli yöntemlerin ve hukuki araçların gelişmesini tetiklemekte; bu gelişme de failleri yeni tekniklere yöneltmektedir. Bu döngüde belirleyici olan, statik bir araç setine değil, sürekli öğrenen ve yöntemini güncelleyen bir yaklaşıma sahip olmaktır. Kripto adli analizinin geleceği, yapay zekâ destekli örüntü tanıma, zincirler arası bütünleşik izleme ve düzenleyici veriyle on-chain istihbaratın giderek daha sıkı entegrasyonu yönünde ilerlemektedir; bu da alanın disiplinler arası niteliğini pekiştirmektedir.

Nihai olarak, blokzincir adli analizinin mahkeme önündeki değeri, teknik doğruluk kadar metodolojik şeffaflığa ve delil zincirinin titizlikle korunmasına bağlıdır. Bu açıdan bakıldığında rapor hazırlayan kişinin görevi, karmaşık bir teknik gerçeği, belirsizliklerini gizlemeden, hukukçunun ve hâkimin anlayabileceği bir netlikte ortaya koymaktır. Bu denge kurulduğunda, açık defterin değiştirilemez hafızası, adaletin en güvenilir tanıklarından biri hâline gelir.

Kaynakça

Chainalysis. (2026). *The 2026 crypto crime report*. Chainalysis Inc. https://www.chainalysis.com/

Elliptic. (2025). *Typologies report: Crypto-asset laundering and cross-chain crime*. Elliptic Ltd.

European Union. (2023). *Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA)*. Official Journal of the European Union.

Federal Bureau of Investigation. (2025, February 26). *Public service announcement: North Korea responsible for the Bybit hack*. FBI.

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

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*, 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*, 1–14. https://doi.org/10.1109/eCRS.2013.6805780

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

TRM Labs. (2025). *The Bybit hack: Following North Korea's largest exploit*. TRM Labs Inc. https://www.trmlabs.com/

burakolgun.com

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

5237 sayılı Türk Ceza Kanunu. (2004). *Resmî Gazete* (Sayı: 25611). (m. 282, suçtan kaynaklanan malvarlığı değerlerini aklama).

5271 sayılı Ceza Muhakemesi Kanunu. (2004). *Resmî Gazete* (Sayı: 25673). (m. 134, bilgisayarlarda arama, kopyalama ve el koyma).

Mali Suçları Araştırma Kurulu (MASAK). (2025). *Kripto varlık hizmet sağlayıcılarına yönelik yükümlülük rehberi*. Hazine ve Maliye Bakanlığı.

Sermaye Piyasası Kurulu (SPK). (2025). *Kripto varlık hizmet sağlayıcılarına ilişkin ikincil düzenlemeler*. SPK.

U.S. Department of the Treasury, Office of Foreign Assets Control. (2022). *Sanctions designation of Tornado Cash*. OFAC.

Europol. (2024). *Cryptocurrencies: Tracing the evolution of criminal finances* (IOCTA spotlight report). European Union Agency for Law Enforcement Cooperation.

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in Bitcoin. *Financial Cryptography and Data Security*, 34–51. https://doi.org/10.1007/978-3-642-39884-1_4

Chainalysis. (2025). *The landscape of seizable crypto assets in 2025*. Chainalysis Inc.

Wilson Center. (2025). *The Bybit heist: What happened and what now?*. Woodrow Wilson International Center for Scholars.

6362 sayılı Sermaye Piyasası Kanunu. (2012). *Resmî Gazete* (Sayı: 28513).

burakolgun.com